UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The Residence Located at 104 Tunbridge Ct., West End, North Carolina

Case No. 1:20MJ76-1

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2252(a)(2)	Receipt/Distribution of Child Pornography
18 USC 2252A(a)(5)(B) and (b)(2)	Possession of Child Pornography

The application is based on these facts:

See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

TYSON HANISH, FBI SPECIAL AGENT

Printed name and title

Sworn to before me and signed in my presence.

Date: 3/4/2020 3:00PM

Judge's signature

City and state: Durham, NC

Joe L. Webster

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF THE RESIDENCE LOCATED AT: 104 TUNBRIDGE CT, WEST END CAROLINA, INCLUDING ANY DETACHED STRUCTURES THERETO, AS WELL AS AUTHORIZING THE FORENSIC EXAMINATION OF COMPUTERS AND RELATED COMPUTER EQUIPMENT.	)	***Case No.*** 1:20MJ76-1

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Special Agent Tyson J. Hanish of the Federal Bureau of Investigation (FBI), a Division of the United States Department of Justice located in Washington D.C., assigned to the FBI Charlotte Division, Fayetteville Resident Agency, make the following statement in support of a request for a search warrant:

1. I have been employed as a Special Agent with the FBI since 2016. I am currently assigned to the Child Exploitation Task Force and I am responsible for conducting investigations of potential violations of federal criminal laws. During my career as an FBI Special Agent I have received training, investigated numerous violations, seized evidence and arrested persons for violations of federal criminal laws.

2. In my capacity as a Special Agent of the FBI, your affiant is authorized to investigate violations of laws and to execute warrants issued under the authority of the United States.

3. This affidavit is submitted in support of an Application for Search Warrant for the residence located at, 104 Tunbridge Ct, West End, North Carolina, as more particularly described in Attachment A, and for the items specified in Attachment B hereto.

4. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of Title 18 U.S.C. § 2252(a)(2) (receipt and distribution of visual depiction involving the use of a minor engaging in sexually explicit conduct); Title 18 U.S.C. § 2252(a)(4)(B)(i) (possession of, with intent to view visual depiction involving the use of a minor engaging in sexually explicit conduct); Title 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); Title 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted to access with intent to view child pornography); and Title 18 U.S.C. § 2252A(3)(B)(ii) (advertised, promoted, presented material with the intent to cause another to believe that the material is child pornography) and are located within 104 Tunbridge Court, West End, North Carolina (hereinafter the "SUBJECT PREMISES"). I submit this application and affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES, as further described in Attachments A and B, incorporated herein by

reference, which is located in the Middle District of North Carolina. Located within the SUBJECT PREMISES to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations. I request authority to search the entire SUBJECT PREMISES, including the residential dwelling and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as contraband and instrumentalities, fruits, and evidence of crime.

5. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent with the FBI.

6. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

STATUTORY AUTHORITY

7. This investigation concerns alleged violations of Title 18 U.S.C. § 2252(a)(2); Title 18 U.S.C. § 2252(a)(4)(B)(i); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of child pornography); 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of child pornography); and 18 U.S.C. § 2252A(3)(B)(ii) (advertising or promotion of child pornography).

8. Title 18, United States Code, Sections § 2252(a)(2) prohibits any person who knowingly receives, or distributes, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

9. Title 18, United States Code, Sections § 2252(a)(4)(B)(i) prohibits any person who knowingly possesses, or knowingly accesses with intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by compute, if the producing of

such visual depiction involves the use of a minor engaging in sexually explicit conduct.

10. Title 18, United States Code, Sections § 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

11. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

12. Title 18, United States Code, Section 2252A(3)(B)(ii) prohibits a person from knowingly advertising, promoting, presenting, distributing or soliciting through the mails, or using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any material or purported material in a manner that reflects the belief, or

that is intended to cause another to believe, that the material or purported material is, or contains a visual depiction of an actual minor engaging in sexually explicit conduct.

DEFINITIONS

13. The following definitions apply to this Affidavit:

14. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

15. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that do not necessarily depict minors in sexually explicit poses or positions.

16. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see Title 18 U.S.C. § 2256(5)).

17. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

18. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between

persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

19. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

20. "Internet Service Providers," (ISPs) as used herein, are commercial organizations that are in business to provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone-based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a username or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records ("ISP records") pertaining to their subscribers (regardless of whether those

subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format.

21. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. Regardless of whether an IP address is dynamically or statically assigned, only one device can be assigned a particular IP address at any one time.

22. "MAC Address," or Media Access Control Address is a unique identifier assigned to a network interface (computer, router, or other device connected to the network) to facilitate communications on the physical network. The local area network (LAN), or other network, uses the MAC address as your computer's unique hardware number. When connected to the Internet or network from your computer, a correspondence table relates your IP address to your computer's physical (MAC) address on the network. A Mac address can be thought of as a device serial number.

23. "Electronic Communication Service Provider ("ESP"), as used herein, is defined in 18 U.S.C. § 2510(15) as any service which provides to users thereof the

ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

24. "Remote Computing Service" ("RCS"), as used herein, is defined in 18 U.S.C. § 2711(2) as the provision to the public of computer storage or processing services by means of an electronic communications system.

25. "Short Message Service" ("SMS"), as used herein, is defined as a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone.

26. The term "computer," as defined in 18 U.S.C. §1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

27. The term "mobile device," as used herein, is defined as a small hand held computing device, having a display screen, and an operating system (OS), with some type of input capabilities (such as a touch screen or a small keyboard), and are typically powered by a battery. Mobile devices are used to run various types of application software, known as apps, as well as communication functions allowing

voice telephone calls, email communications, SMS and MMS functions. Smart cellphones, tablets, and PDAs are popular forms of mobile devices. Most handheld devices are often typically equipped with Wi-Fi, Bluetooth and GPS capabilities, allowing the device to connect to the Internet and other devices (such as a vehicle or a microphone headset) or can be used to provide Location-based services (like mapping and directional applications). Most mobile devices typically have an internal camera for taking and recording still image and video files, which are then stored within the memory of mobile device.

28. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

29. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to

restrict access to computer hardware (including, but not limited to, physical keys and locks).

30. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

31. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

32. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

33. "VPN service," as used herein, is an acronym for Virtual Private Network (VPN) service. A VPN service extends a private network across a public network,

and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. VPN services allow employees to securely access a corporate intranet while located outside the office. Individual Internet users may secure their internet transactions with a VPN, to circumvent geo-restrictions and censorship, or to connect to internet while masking their personal identity and location information, like their IP address.

BACKGROUND AND USE OF THE "KIK MESSENGER"

34. Kik Messenger, also known as "Kik," is a popular free instant messenger application (app) for mobile devices (i.e. smart cell phones, tablets, iPods, etc.) from the Canadian company, Kik Interactive, which was founded in 2009. Kik is available on several mobile device platforms including, iOS, Android, and Windows Phone operating systems. The Kik application can be located through Google's, "Play Store," and Apples, "App Store." The Kik application utilizes the internet connection through the mobile devices' data plan or through Wi-Fi, to transmit and receive messages, photos, videos, sketches, mobile webpages, and other content transmitted by through the Kik application. Kik allows its users to register an user account without providing a telephone number, and prevents users from being located on the service through any information other than their chosen unique Kik username. According to Kik Interactive, Kik Messenger has approximately 300 million registered users, and is used by approximately 40 percent of United States teenagers.

35. Based on Kik's website, (https://www.kik.com/about/), "Kik has become the best way to connect with friends, no matter where you meet them. And unlike

other messengers, Kik uses usernames - not phone numbers - as the basis for Kik accounts, so our users are always in complete control of who they talk to on Kik. But Kik isn't just about our users chatting with their friends. Our tools let our partners talk to and share cool content with our users, and track the results. Our developer tools help developers optimize and distribute their content on Kik."

36. After locating the Kik application and downloading the application to the mobile device, the application requests permission to access the following data on the mobile device during the installation process; In-app purchases, Identity, contacts, Location, Photos/Media/Files, camera, Microphone, Device ID & call information. Once given permission by the user, the Kik application installs itself on the mobile device. After installing the Kik app on the mobile device and initializing the Kik application for the first time, the potential user is required to establish a Kik account and is prompted to select the "SIGN UP" option. While establishing a Kik account, the potential user is prompted to provide information, including the user's "First Name," "Last Name," and "Birthday." The potential user is prompted to create a, "Kik Username," (which is the only information that is required to be unique,) and is prompted to provide an "Email address." The information provided by the potential user is used to establish a Kik account; however, this user information is not verified and the information can be completely fictitious (except for the uniqueness of the Kik username). A "verification email" is sent by Kik to the user's provided email address and the user is prompted to verify the email address. Verification of the user's email address is not required and does not prevent the user from utilizing the application

if not verified. The potential Kik user is prompted to provide a user profile picture, which can either be taken using the mobile device's camera feature or uploaded from the device photo gallery. However, the lack of a profile picture does not prevent the user from utilizing the application. The Kik username is created by the user and is the only information that is required to be unique.

37. At the completion of the account registration, the user is allowed to start communicating with other Kik users. Searching for specific Kik users can only be performed using the Kik user's registered "username;" searches by phone number or email address cannot be performed. Entering the unique Kik username through the application's search field yields potential matches in which the user simply selects the Kik user to start communicating with that specific user.

38. In today's world where mobile phones are the technology of choice for millions of people to communicate, chat applications like Kik Messenger are often used to communicate with others, and on occasions are used during the commission of crimes, like the online harassment and bullying of juveniles, and the sexual exploitation of minors. Mobile devices which utilize social media and communication applications, store, or "cache," certain data from the social media or communication applications directly on the mobile device and this data can be recovered by a forensic expert. The Kik Messenger application is no different.

39. For both iOS and Android devices, most Kik artifacts relevant to criminal investigations are stored within specific databases located in specific locations on the mobile devices. These databases store details concerning the Kik users' contacts,

messages, and attachments sent and received through the Kik Messenger application. These databases contain such data as the usernames and display names for each contact, but are not limited to this type of information. The Kik username is a unique identifier for each and every Kik user and this type of data is valuable in criminal investigations. The Kik contact database can also contain profile picture links and timestamps, as well as group and block lists. This data can be recovered from the mobile device by trained computer experts.

40. Messages, including any attached image files, are stored within a specific location on the mobile device, depending on the device used. As Kik stores all of its data in this specific location within the mobile device, in an unencrypted format, there is a good chance that the entire messaging history, if not a partial message history, can be recovered by trained computer experts and used during investigations.

41. Users sometimes delete their conversation histories by clearing the Kik Messenger logs. However, since the Kik messaging databases are not wiped or erased immediately (depending on the operating system of the mobile device), these deleted records end up being stored in a specific location in a specific format on the mobile device. These deleted records may be kept for a period of time until the database reclaims the space to store new records. A forensic expert has the ability to recover such records which could prove useful in various investigations.

42. Sometimes, a user will attempt to destroy evidence by deleting the database file completely. While there is nothing that can be done to recover this

information from an iOS device (the operating system does not allow for the recovery of anything that has been deleted), carving Android and chip-off dumps may return an amazingly high amount of deleted evidence.

BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND E-MAIL

43. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

44. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

45. The development of computers has added to the methods used by child pornography collectors to interact with, and sexually exploit children. Computers

serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

46. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto, and stored by a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, satellite, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

47. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

48. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

49. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Electronic Service Providers, such as Yahoo! and Goggle, as well as remote storage accounts like Dropbox and MediaFire, among many others. These online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet (including smart phones tablets, iOS devices, and any other device that can access the internet) and access these stored images with ease. In most cases, even in cases where a remote storage service is used to store images of child pornography, evidence of the child pornography can still be found on the user's computer.

50. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, e.g., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web

cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

51. If a saved image is deleted from a computer, the image is not truly removed from the computer's hard drive until it is completely overwritten with new data. Often times, deleted images can still be located on the computer's unallocated space of the hard drive. This unallocated space is held in reserve by the computer's operating system until a new file is created and the space is needed for storage. A digital forensic examiner can often recover deleted files from the unallocated space which have not yet been overwritten by the computers operating system in the process of saving new data. In addition, if the computer user only views an image through the Internet browser but does not save the image to their computer, the image could still be recovered from the hard drive of the computer in a specific designated folder of the computer's operating system, as long as the data had not been overwritten.

52. With the advent of mobile devices (i.e. "smart" cell phones, tablets, PDAs ...) which can access the internet through a multitude of different applications, individuals engaged in the viewing, storing, and trading of child pornography have been able to access, store, and trade these images using their cell phones. Mobile devices are essentially mini-handheld computers with most of (or all of) the

functionality of a traditional computer. Mobile devices can utilize applications for remote storage services (like Dropbox, MediaFire, and OneDrive accounts) to access, view, store, and share digital files with others, including images of child pornography. Mobile devices can also be used to communicate with others through various chat applications, to including video chat and image sharing applications.

DETAILS OF INVESTIGATION

53. Based upon the investigation to date, I believe there is probable cause to believe that a search of the SUBJECT PREMISES will discover evidence, fruits, and/or instrumentalities of crimes including violation of Title 18 U.S.C. § 2252(a)(2) (receipt and distribution of visual depiction involving the use of a minor engaging in sexually explicit conduct); Title 18 U.S.C. § 2252(a)(4)(B)(i) (possession of, with intent to view visual depiction involving the use of a minor engaging in sexually explicit conduct); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of child pornography); 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of child pornography); and 18 U.S.C. § 2252A(3)(B)(ii) (advertising or promotion of child pornography), and these assets are subject to forfeiture under 18 USC § 2253.

54. My belief is based upon the following facts and circumstances:

55. The affiant certifies that the Federal Bureau of Investigation is conducting a criminal investigation involving the receipt, possession, advertisement, promotion and distribution of child pornography, in violation of federal laws, including but not limited to, Title 18 U.S.C. § 2252(a)(2) (receipt and distribution of visual depiction involving the use of a minor engaging in sexually explicit

conduct); Title 18 U.S.C. § 2252(a)(4)(B)(i) (possession of, with intent to view visual depiction involving the use of a minor engaging in sexually explicit conduct); Title 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); Title 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted to access with intent to view child pornography); and Title 18 U.S.C. § 2252A(3)(B)(ii) (advertised, promoted, presented material with the intent to cause another to believe that the material is child pornography).

56. On February 9, 2020, Online Covert Employee (OCE), hereinafter OCE, who is a member of the FBI Child Exploitation and Human Trafficking Task Force (CEHTTF)in Albany, New York, was connected to the internet in an online undercover capacity from an internet capable device located in Albany, NY. A software program was utilized to record the online activity, chats, and images identified within KiK. OCE was located in a KiK group titled "Daught Phuck" "#daughtphuck". Based on OCE's experience and information gathered from other sources, this particular chat room is frequented by individuals who have a sexual interest in children and incest. OCE was in this public forum and provided OCE's KiK screen name.

57. On February 9, 2020, an individual with the KiK profile name "naughtydaddy95", using the screen name "Jim John", entered kik group "Daught Phuck" "#daughtphuck" at approximately 3:50pm. OCE posted a

picture of his purported nine (9) year old daughter with caption "Fully active she's 9". Shortly thereafter naughtydaddy95 private messaged (PM) OCE. naughtydaddy95 initiated contact with OCE who had no prior contact with naughtydaddy95.

58. All text communications between naughtydaddy95 and OCE were recorded. The below is a summary of the KiK chat session. It is not intended to be a verbatim account and does not memorialize all statements made during the chat. Communications by the parties during the chats were memorialized and provided to the case file. The recordings capture the actual text conversation.

59. OCE stated OCE loved naughtydaddy95's profile picture. naughtydaddy95 sent an image of a clothed female who appears to be approximately nine (9) years old and stated it was naughtydaddy95's youngest daughter. OCE asked if naughtydaddy95 was sexually abusing her to which naughtydaddy95 replied "we tease and play but I'm still nervous". naughtydaddy95 then stated his nine (9) year old daughter "likes to grind on my lap and get me hard and just smiles at me." naughtydaddy95 sent two more images of his alleged daughter, both are fully clothed.

60. naughtydaddy95 asked OCE "Got any bikini or pantie pics". OCE stated OCE required a picture of naughtydaddy95 with his daughter and then a camera picture of naughtydaddy95. naughtydaddy95 sent an image of an adult male, fully clothed, standing between two female children, fully clothed. The female on the right appears to be one in the same as the female child previously described

above. naughtydaddy95 then sent a camera picture, indicating the picture was taken within the kik application, at that very moment, of his face. The camera face picture sent by naughtydaddy95 and the male's face in the image with the two female children appear to be one in the same.

61. naughtydaddy95 then sent an image of a young female doing a head stand with her legs spread. The female is wearing white underwear, the focal point of the image is of the females clothed vagina, naughtydaddy95 stated "I love young, wink emoji". naughtydaddy95 stated his favorite age is eight (8) to thirteen (13). naughtydaddy95 then sent an image, the image is of two females on a hammock, both of their genitals are exposed. The one female is performing oral sex on the other female. Both females appear to be ten (10) to fourteen (14) years old.

62. naughtydaddy95 then sent a video of what appears to be an eight (8) to ten (10) year old female who removes all of her clothing and exposes her anus and vagina.

63. naughtydaddy95 stated: "No, I'm just scared to go farther then I have so far just rubbing her in her sleep and letting her watch me jack off I want more just scared I know she wants more just not sure how to go about it, we have had a couple hot make out sessions where I have put her hand on my cock and let helped her stroke it".

64. naughtydaddy95 stated "So do you ever jack off in her panties? I can't help myself but use mines". naughtydaddy95 sent an image of a young female child in a cheerleader uniform. The female appears to be the same female previously described as standing next to the adult male above. naughtydaddy95 then sent

two images of female's underwear in an dresser draw via camera picture, indicating the picture was taken within the kik application, at that very moment.

65. naughtydaddy95 sent an image of a female approximately six (6) to (8) years old wearing a bikini with her legs spread, the female's vagina is the focal point of the image. naughtydaddy95 stated it was "Hot random".

66. naughtydaddy95 sent an image of an adult male and female standing together indicating it was him and his wife. The male appears to be one in the same as the kik camera picture of the adult male's face and also the same adult male standing with the two female children.

67. On February 20, 2020 administrative subpoena was obtained and served to the Electronic Service Provider (ESP), Kik Interactive, Inc., requesting the subscriber information and IP connectivity logs for the SUBJECT KIK ACCOUNT, naughtydaddy95. Kik Interactive, Inc. responded to the administrative subpoena and provided the requested information.

68. Based on the results provided by Kik Interactive, Inc., the following information was associated with the SUBJECT KIK ACCOUNT, 'naughtydaddy95':

First Name: Jim

Last Name: John

E-Mail: johndonjim269@yahoo.com (unconfirmed)

Username: naughtydaddy95

REGISTRATION_CLIENT_INFO device-type=iPhone

REGISTRATION_CLIENT_INFO model=iPhone

USER_LOCATION US (tz: America/New_York, ip: 65.191.166.24)

69. Based on the client information provided by Kik Interactive, Inc., the mobile device associated with the SUBJECT KIK ACCOUNT, is believed to be an iPhone.

70. Kik Interactive, Inc. also provided the IP connectivity logs of the SUBJECT KIK ACCOUNT. These logs record at what time and from what IP address a Kik user accesses their Kik account. During the affiant's review of the IP connectivity logs of the SUBJECT KIK ACCOUNT, it was noted that the user of the SUBJECT KIK ACCOUNT logged into the SUBJECT KIK ACCOUNT on multiple dates and times from different IP addresses. Based on the affiant's experience investigating Internet crimes, it is typical to observe multiple logins to social media applications or email accounts on multiple dates and times from different IP addresses due to portability of mobile devices (i.e. smartphones and tablets, and other mobile devices).

71. During the affiant's review of the IP connectivity logs, it was observed that many of the login IP addresses employed by the user were assigned to the mobile cell phone data provider, Verizon Wireless, and a residential Internet Service Provider, Time Warner Cable (Charter Communications, Inc.).

72. On February 20, 2020, an administrative subpoena was obtained and served to the ISP, Charter Communications, Inc., for the subscriber information related to the IP address (65.191.166.24) utilized by the SUBJECT KIK ACCOUNT on the specified dates and times.

73. Based on the results provided by Charter Communications, Inc., the following information was associated with the aforementioned IP addresses:

Subscriber Name: Robert Clark

Subscriber Address: 104 Tunbridge Ct, West End, NC

Account Number: 308188904

74. A search with the North Carolina Department of Motor Vehicles shows that Robert Andrew Clark, date of birth 10/23/78 has a North Carolina driver's license number 39005551 and has the 104 Tunbridge Ct., West End, North Carolina listed as his residence. An FBI Task Force Officer observed the SUBJECT PREMISES and took digital photographs of the residence for identification purposes.

CHARACTERISTICS OF CHILD PORNOGRAPHY COLLECTOR

75. During the affiants investigations into sexually related crimes, it was noted that a majority of individuals view pornography on their computers (or mobile devices) via the internet, and often store copies of images in a way to allow them easy access to the images, including thumb drives, external hard drives, web storage sites, and other digital storage devices. Through my training and experience working cases involving child pornography, and through consulting with others experts in the field, I have learned that illegal contraband, such as child pornography and other materials like child erotica and incest literature, are typically collected, stored, and distributed by individuals that engage in this type

of illegal activity. This type of contraband (collected child pornography) is not "used up" as are other types of contraband, such as alcohol or drugs. Contraband of this type can and is usually stored for indefinite amounts of time by the possessors of this illegal contraband. Users who collect child pornography are sexual aroused by images of child pornography. Child pornography is not readily available commercially in the United States or most other countries as is adult pornography. Child pornography users are forced to obtain their pornographic media from other sources. Once users collect these images and add them to their collections, the users often do not dispose of these images. These individuals often hide their viewing/storage of pornographic images from their loved ones and other household members. Through my training and experience, and through consultation with other experts, it is known that in many instances these types of files have been found stored for years and transferred from and between storage mediums, storage devices, and from the user's old computer to the user's new computer.

76. The affiant also noticed pornography users view pornography that mirrors their sexual attraction to a particular phenotype. For example, if a person is sexually attracted to petite females with brown hair, the majority of the pornographic images they would view would consist of petite females with brown hair. If a person is sexually attracted to the soles of a woman's foot, the majority of images they would view would consist of the sole of women's feet. If a person is sexually attracted to children, the majority of images they view would consist of lewd and

lascivious images of children or of children engaged in sexual contact. With this said most pornography users have more than one sexual fetish and will view images to satisfy all or most of their fetishes. The theme of the collections will be evident upon examining the images collected by the pornographic viewer or stored on their devices.

77. I have personally been involved in the execution of search warrants relating to child pornography investigations. I have personally interviewed offenders. I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 USC § 2256) in all forms of media including computer media. I have read publications related to the investigations of sexual exploitation of children. I have consulted with other law enforcement officers who investigate the sexual exploitation of children. Based on my training and experience, I know that:

78. The majority of individuals who collect child pornography are persons who have a sexual attraction to children.

79. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital images or other images for their own sexual gratification.

80. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collections of illicit materials from discovery. They almost always

maintain their collections in the privacy and security of their own homes or other secure locations.

81. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and seemingly anonymous fashion.

82. Child pornography is not readily available in retail establishments; accordingly, individuals who wish to obtain child pornography commonly do so by ordering it from abroad or by discreet contact with other individuals who have it available, or by locating the images online through various websites.

83. Mobile digital communications devices have increasingly become used by offenders to access the Internet in efforts to search for child pornography, to obtain it directly or via a tethering function of the digital device (such as a smart phone or portable cellular data hot spot or USB cellular modem), for communicating with other offenders as well as with victims, and for accessing remote online storage sites (such as uploading or downloading saved files of child pornography) as well as using such devices as a portable repository for stored child pornography.

84. Individuals who collect child pornography tend to do so repeatedly, and do not easily abandon their collections or their collecting conduct.

SEARCH AND SEIZURES OF COMPUTERS

85. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following

techniques (the following is a non-exclusive list, as other search procedures may be used):

a) examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b) searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c) surveying various file directories and the individual files they contain;

d) opening files in order to determine their contents;

e) scanning storage areas;

f) performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storages areas exist that are likely to appear in the evidence described in Attachment B, and / or;

g) performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

SEARCH METHODOLOGY TO BE EMPLOYED

86. Based upon my training, experience, and information obtained from other law enforcement officials familiar with child exploitation crimes, I know that when an individual uses a computer to download child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage device for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage device for evidence of crime. From my training and experience, I know that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of internet discussions about the crime; and other records that indicate the nature of the offense. There is probable cause to believe that the contraband images (child pornography) will be located on the hard drives of the suspect's computers and on any digital media storage devices located within the residence mentioned in Attachment A, which will constitute evidence, fruits, and instrumentalities of child exploitation crimes, including the receipt, distribution, and/or collection of child pornography.

87. Based upon my knowledge, training and experience, I know that searching for information stored in computers often requires agents to seize most or all electronic storage devices to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is often necessary to ensure

the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine those storage devices in a laboratory setting, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the laboratory setting. This is true because of the following:

88. The process of searching the digital files contained within digital media storage devices at the scene can take a long time to complete. To be certain the digital storage devices in question do not contain any contraband materials, law enforcement officers would have to examine every one of what may be thousands of files on a digital storage device. This process could take a long time. Taking too much time to conduct the search would not only impose a significant and unjustified burden on police resources, it would make the search more intrusive. Police would have to be present on the suspect's premises while the search was in progress therefore denying the suspect(s) access to their home or business for an extended amount of time. If the search took hours or days, the intrusion would continue for that entire period, compromising the Fourth Amendment value of making police searches as brief and non-intrusive as possible.

89. Technical requirements for searching computer systems for criminal evidence sometimes requires highly technical processes requiring expert skill and properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to

analyze the system and its data. In any event, however, data search processes are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis.

90. In light of these concerns, I hereby request the Court's permission to seize the computer hardware (and associated peripherals) that are believed to contain some, or all of the evidence described in the warrant, and conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.

CONCLUSION

91. Based upon the foregoing, I submit that there is probable cause to believe that the residence described in Attachment A, contains evidence of violations of United States Code 18, Sections 2252A and 2252.

92. WHEREFORE, I respectfully request that a search warrant be issued authorizing your deponent or any law enforcement agents to search of the SUBJECT PREMISES, located at 104 Tunbridge Ct., West End, North Carolina, within the Middle District of North Carolina, and seize and search the aforementioned computer hard drives, computer equipment, and any other

evidentiary items, detailed in Attachment B, all of which constitute evidence, fruits, and instrumentalities of violations of Title18, United States Code, Sections 2252A and 2252.

93. I assert that public disclosure of the existence of this search warrant affidavit and all accompanying materials at this juncture could jeopardize the government's ongoing investigation in this case and therefore I request this affidavit and all accompanying material be sealed until further order of this Court.

Respectfully submitted,

Tyson Hanish, Special Agent
Federal Bureau of Investigations

On this 4th day of March 2020, Tyson Hanish appeared before me, was placed under oath, and attested to the contents of this Affidavit.

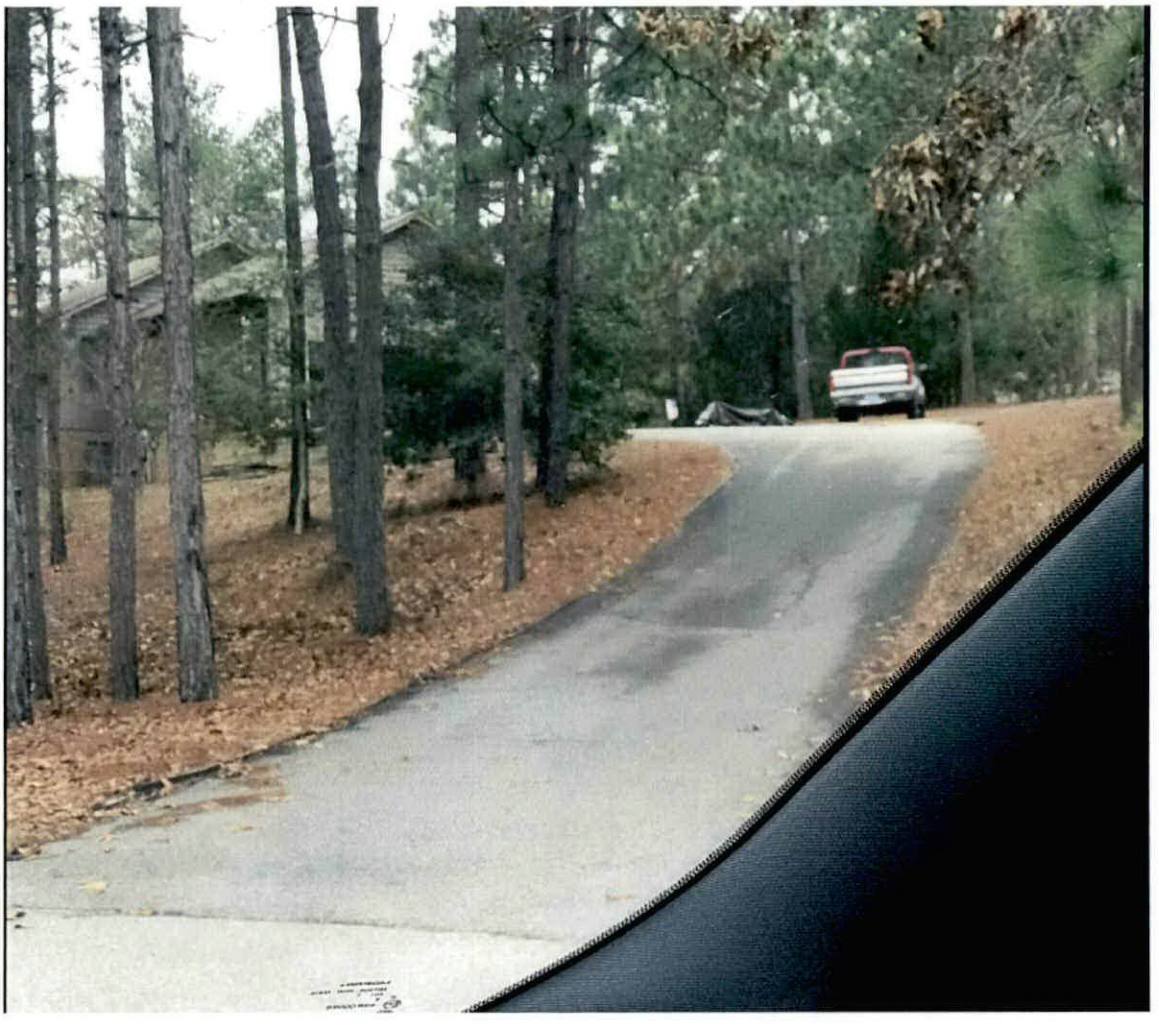
Joe L. Webster
United States Magistrate Judge

Premises to Be Searched

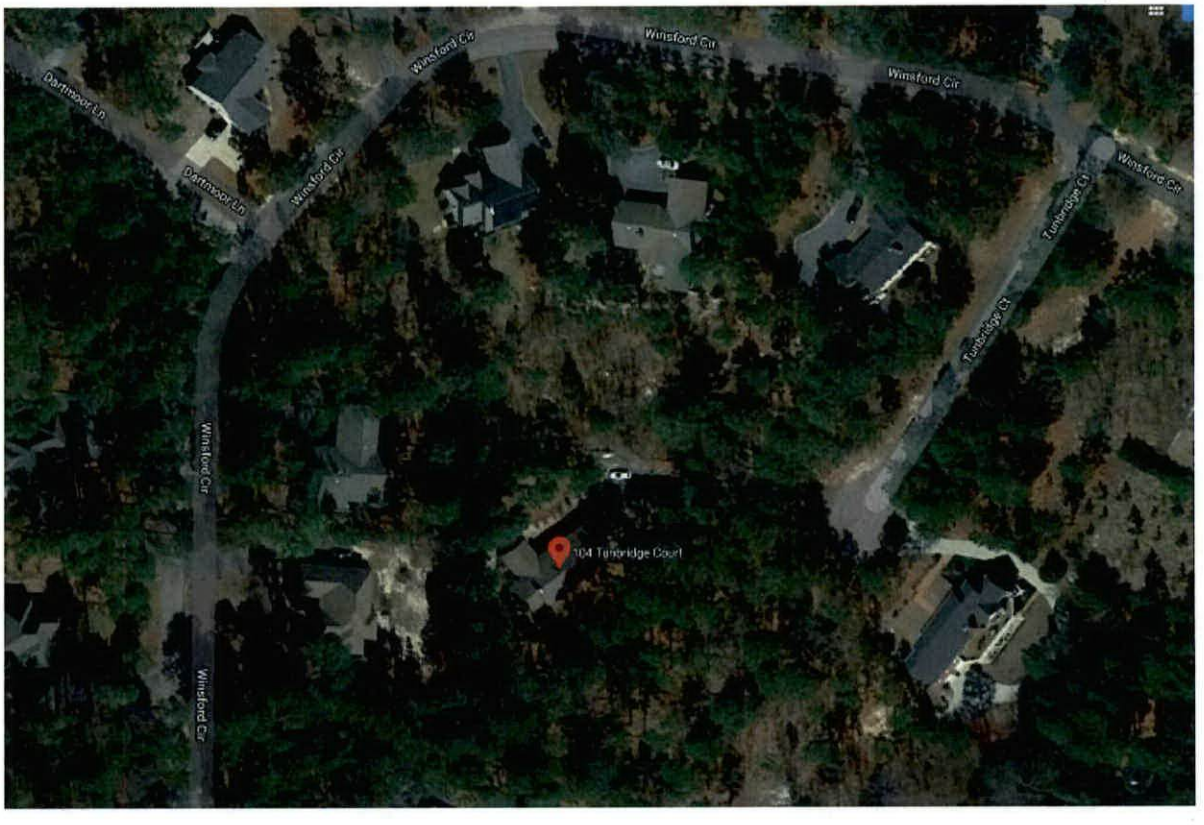
The residence located at **104 Tunbridge Ct., West End, NC 27376**, is situated in Moore County within the middle district of the state of North Carolina. The residence is a single-family structure with a long driveway. The house is in a wooded area.

An area map and photographs of the premises are incorporated herein.

Subject Premises:



Satellite and overhead map of area:


Winsford Cir
Winsford Cir
Winsford Cir
Dartmoor Ln
Dartmoor Ln
Winsford Cir
Winsford Cir
Tunbridge Ct
Tunbridge Ct
Winsford Cir
Winsford Cir
704 Tunbridge Court

ATTACHMENT B.

ITEMS TO BE SEARCHED FOR AND SEIZED

This warrant authorizes (i) the search of the property identified in **Attachment A** for only the following and (ii) authorizes the seizure of the items listed below only to the extent they constitute the following:

(a) evidence of violations of Title 18 U.S.C. §§ 2252 and 2252A, Sexual Exploitation of Minors and Material Constituting Child Pornography; or

(b) any item constituting contraband due to the subject violations, fruits of the subject violations, or other items possessed whose possession is illegal due to the subject violations; or

(c) any property designed for use, intended for use, or used in committing any subject violations.

Subject to the foregoing, the items authorized to be seized include the following:

1. Computer(s), computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, video recording devices, video recording players, monitors and or televisions, and data were instrumentalities of and will contain evidence related to this crime. The following definitions apply to the terms as set out in this affidavit and attachment:

a) Computer Hardware

Computer hardware consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, **telephones and other mobile or portable devices**, video gaming systems, tablets, music/media

players, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

b) Computer Software

Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

c) Documentation

Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

d) Passwords and Data Security Devices

Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware

may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

2. Any and all notes, documents, records, or correspondence pertaining to child pornography as defined under Title 18, United States Code, § 2256(8).

3. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by use of the computer and/or for the purpose of distributing child pornography.

4. Any and all correspondence identifying persons transmitting, through interstate commerce including by United States Mails or by computer, any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, § 2256(2).

5. Any and all records, documents, invoices and materials that concern any accounts with any Internet Service Provider.

6. Any and all cameras, film, or other photographic equipment.

7. Any and all visual depictions of minors.

8. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States Mails or by computer, and visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, § 2256(2).

9. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, § 2256(2).

10. Any and all documents, records, or correspondence pertaining to occupancy at **104 Tunbridge Ct., West End, North Carolina, 27376.**

11. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, § 2256(2).

12. Any of the items described in paragraphs 1 through 11 above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment, including floppy diskettes, fixed hard disks, or removable hard disk cartridges, software or memory in any form.